Stephen G. Larson (SBN 145225)
slarson@larsonllp.com
Paul A. Rigali (SBN 262948)
prigali@larsonllp.com
LARSON LLP
555 South Flower Street, 30th Floor
Los Angeles, California 90071
Telephone:(213) 436-4888

John J. Nelson (SBN 317598)
jnelson@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941

Attorneys for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

JESSE SCHMIDT and STEVEN JANTZEN, individually, and on behalf of all others similarly situated, Plaintiffs, vs. LOANDEPOT, INC., Defendant.	Case No.: 8:24-cv-00200 **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Jesse Schmidt and Steven Jantzen, individually, and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant LoanDepot, Inc. ("Defendant" or "LDI"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations on information and belief, except as to their own actions, which are made on personal knowledge, the investigation of counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of the recent targeted ransomware attack and data breach ("Data Breach") on LDI's network that resulted in unauthorized access to the highly sensitive data of roughly 16.6 million individuals.[1] As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. Upon information and belief, the specific information compromised in the Data Breach includes, but is not limited to, personally identifiable information ("PII"), such as full names, dates of birth, addresses, Social Security numbers, and tax identification numbers.

3. Upon information and belief, up to and through January 2024, Defendant obtained the PII of Plaintiffs and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant LDI's network, from which unauthorized actors used an extraction tool to retrieve sensitive PII belonging to Plaintiffs and Class Members.

4. Plaintiffs' and Class Members' PII—which were entrusted to

[1] https://media.loandepot.com/news-releases/press-release-details/2024/l-oanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last accessed January 23, 2024).

Defendant, their officials, and agents—were compromised and unlawfully accessed due to the Data Breach.

5. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiffs and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

6. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network, IT systems, and integrated service that housed Plaintiffs' and Class Members' PII.

8. Defendant's failure to safeguard its clients PII is particularly heinous in light of the fact that Defendant suffered a separate, prior data breach in August 2022 about which it notified its customers nearly a year later in May 2023.

9. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks to Plaintiffs and Class Members will remain for their respective lifetimes.

10. Defendant failed to provide timely, accurate and adequate notice to Plaintiffs and Class Members. Plaintiffs' and Class Members' knowledge about the PII Defendant lost, as well as precisely what type of information was unencrypted

and in the possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn impacted persons immediately upon learning of the Data Breach.

11. As remediation for allowing Plaintiffs' and Class Members' PII to be acquired by an unauthorized third-party, Defendant has stated that "[t]he Company will notify [the affected] individuals and offer credit monitoring and identity protection services and no cost to them."[2] To date, Defendant has not contacted or offered any remediation to the victims of this Data Breach, but this assurance serves as tacit acknowledgement of the harm and elevate risk that 16.6 million individuals now face as a result of Defendant's acts and omissions.

12. Indeed, armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present, heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against identity theft for the rest of their lives.

14. Plaintiffs and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. By their Complaint, Plaintiffs seek to remedy these harms on behalf of

[2] *Id.*

themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

16. Accordingly, Plaintiffs bring claims on behalf of themselves and the Class for: (i) negligence, (ii) invasion of privacy and (iii) unjust enrichment, (iv) violations of the California Unfair Competition Law, (v) violations of the Florida Deceptive an Unfair Trade Practices Act; and (vi) declaratory judgment and injunctive relief. Through these claims, Plaintiffs seek, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

PARTIES

17. Plaintiff Jesse Schmidt is a natural person, resident, and citizen of Port St. Lucie, Florida, where he intends to remain. He is a Data Breach victim, having applied for a loan from Defendant in or about November 2023.

18. Plaintiff Steven Jantzen is a natural person, resident, and citizen of Crowley, Texas, where he intends to remain. He is a Data Breach victim, having applied for a loan from Defendant in or about November 2023.

19. Defendant LoanDepot, Inc, is a provider of mortgages and lending services. LDI is headquartered at 6561 Irvine Center Drive, Irvine, CA 92610.

20. Defendant LDI is an affiliate or parent company of numerous other companies, including but not limited to: LD Holdings Group LLC, loanDepot.com, LLC, LD Settlement Services, LLC, American Coast Title Company, Inc., melloInsurance Services, LLC, Closing USA of Alabama, LLC, Closing USA LLC, Closing USA of Arkansas, LLC, Commercial Agency USA, LLC, Closing USA of Delaware, LLC, Closing USA of Utah, LLC, mello Holdings, LLC, mello Home Services, LLC, mello Home, Inc., MTH Mortgage, LLC, MSC Mortgage, LLC, Tri Pointe Connect, LLC, Day One Mortgage, LLC, loanDepot-FB Mortgage, LLC (d/b/a Farm Bureau Mortgage), Heartwood Mortgage, LLC, BRP Home Mortgage, LLC, Henlopen Mortgage, LLC, LGI Mortgage Solutions, LLC, NHC Mortgage,

LLC.

21. Defendant LDI is a corporation formed in Delaware and registered in good standing in California. According to the California Secretary of State, Defendant's California Registered Corporate Agents are Jackson Yang, Gabriela Gonzalez, Jeffrey Kurtz, Jennifer McLaughlin, Jaclyn Wright, Adam Saldana, Mackenzie Hibler, Alvine Sayre, Jessice Wittry, Angela Castillo, Ashley Sims, and Emily Rendon.

JURISDICTION AND VENUE

22. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including Plaintiffs, are citizens of a different state than Defendant, there are more roughly 16.6 million putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

23. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and in this District through its headquarters, offices, parents, and affiliates.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal places of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND FACTS

A. Defendant's Businesses

25. Defendant LDI is the country's fifth largest retail mortgage lender and the second largest nonbank retail originator. Since its founding in 2010, Defendant has provided more than $275 billion in lending. LDI currently employes more than

6,000 individuals and services more than 27,000 customers each month.[3]

26. On information and belief, Defendant maintain the PII of customers, employees, and others, including but not limited to:

a. name, address, phone number and email address;

b. date of birth;

c. demographic information;

d. Social Security number;

e. tax identification number;

f. financial information;

g. medication information;

h. health insurance information;

i. photo identification;

j. employment information, and;

k. other information that Defendant may deem necessary to provide its services.

27. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

28. Because of the highly sensitive and personal nature of the information Defendant acquires, stores, and has access to, Defendant, upon information and belief, promised to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to medical care and treatment; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs'

[3] https://www.loandepot.com/about (last accessed January 23, 2024)

and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

30. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

31. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

B. Defendant Fails to Safeguard Consumer PII

32. On or around January 8, 2024, Defendant LDI posted the following online:

> LoanDepot is experiencing a cyber incident. We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers and we are focused on resolving these matters as soon as possible.[4]

33. Over the next several days and weeks, Defendant continued to intermittently post updates to its website alerting customers when its various subsidiaries' payment portals were reactivated.[5] On or about January 22, 2024, Defendant posted the following statement in response to the Data Breach:

> The Company has been working diligently with outside forensics and

[4] https://loandepot.cyberincidentupdate.com/ (last accessed January 23, 2024)

[5] https://loandepot.cyberincidentupdate.com/ (last accessed January 23, 2024)

security experts to investigate the incident and restore normal operations as quickly as possible. The Company has made significant progress in restoring our loan origination and loan servicing systems, including our MyLoanDepot and Servicing customer portals.

Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.

"Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact to our customers," said LoanDepot CEO Frank Martell. "The entire LoanDepot team has worked tirelessly throughout this incident to support our customers, our partners and each other. I am pleased by our progress in quickly bringing our systems back online and restoring normal business operations."

"Our customers are at the center of everything we do," said Jeff Walsh, President of LDI Mortgage. "I'm really proud of our team, and we're glad to be back to doing what we do best: enabling our customers across the country to achieve their financial goals and dreams of homeownership."

The Company is committed to keeping its customers, partners and employees informed and will provide any additional operational updates

on our microsite at loandepot.cyberincidentupdate.com.[6]

34. To date, Defendant's investigation has determined that the private information of roughly 16.6 million customers and other affiliated individuals was accessed and compromised by an unauthorized user on or about January 8, 2024.

35. It is likely the Data Breach was targeted at Defendant due to its status as a financial services provider that collects, creates, and maintains sensitive PII.

36. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the PII of Plaintiffs and the Class Members.

37. While Defendant LDI stated in its public notice it would directly notify the affected individuals and that it is committed to keeping the victims informed, upon information and belief Defendant has not yet directly notified Plaintiffs or Class Members.

38. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiffs' PII was stolen in the Data Breach. Plaintiffs further believe their PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals.

39. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

40. In response to the Data Breach, Defendant LDI admits it worked with external "security experts" to determine the nature and scope of the incident and purports to have taken steps to secure the systems. Defendant LDI admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiffs' and Class Members' PII going forward.

41. Because of the Data Breach, data thieves were able to gain access to

[6] https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last accessed January 23, 2024)

Defendant's private systems on January 8, 2024, and were able to compromise, access, and acquire the protected PII of Plaintiffs and Class Members.

42. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

43. Plaintiffs and the Class Members reasonably relied (directly or indirectly) on Defendant's sophistication to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

44. Plaintiffs' and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The risks to Plaintiffs and Class Members will remain for their respective lifetimes.

C. The Data Breach was a Foreseeable Risk and Defendant Knew or Should Have Known That They Were a Target of Cybercriminals

45. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the mortgage industry and other industries holding significant amounts of PII preceding the date of the breach.

46. In light of recent high profile data breaches at other financial services companies, Defendant knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups.

47. Defendant LDI knew or should have known that these attacks were common and foreseeable.

48. Indeed, LDI itself was subject to a separate data breach in August 2022, which LDI waited nearly a year (until May 2023) to disclose to its customers,

49. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[7]

50. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals

51. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

52. In acknowledgement of these significant risks, LDI publishes its "Privacy Policy to customers and potential customers on its website In that policy, and as an inducement to customers providing personally identifiable and other confidential information, LDI has made certain representations and promises including the following:

> "Safeguarding Personally Identifiable Information
>
> - We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.
> - We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to your files,

[7] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.

- We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.

LoanDepot Security Policy

loanDepot takes steps to safeguard your personal and sensitive information through industry standard physical, electronic, and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and servers with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a high-ranking manager.

Sharing Information with Companies That Provide Services for Us

We share personally identifiable information about you, as required or permitted by law, with third parties, such as service providers who assist us in the in the administration, processing, closing, settlement, title or other insuring, servicing, and sale of your loan, or other service providers who assist us in fulfilling products and services for you. These third parties include among others, loan origination system providers, lenders, title companies, appraisers, insurance companies, real estate companies, underwriting services, notary services, processing services, printing companies, document providers, software and technology providers, fraud detection companies, marketing services providers, and purchasers of loans. Our policy is to require third party service providers to enter into confidentiality agreements with us, prohibiting them from using any personally identifiable information they obtain for any other purpose other than those for which they were retained or as required by law.

53. In light of the known risks, LDI failed to act to implement reasonable and readily available data security procedures and practices to protect against disclosure of its customers' highly confidential information disregarding and in violation of its representation and legal obligations to its customers and state law.

D. Defendant Fails to Comply with FTC Guidelines

54. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[8] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[9]

56. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to

[8] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 23, 2023).

[9] *Id*.

confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. These FTC enforcement actions include actions against mortgage lenders and partners like Defendant.

59. Defendant failed to properly implement basic data security practices.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

61. Defendant was at all times fully aware of their obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from their failure to do so.

62. Defendant's failure implement reasonable data security was directly contrary to the representations made to its customers in its Privacy Policy and constitute material misrepresentations.

E. Defendant Fails to Comply with Industry Standards

63. As shown above, experts studying cyber security routinely identify mortgage lenders and partners as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

64. Several best practices have been identified that at a minimum should be implemented by mortgage lenders like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

65. Other best cybersecurity practices that are standard in the mortgage

industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

66. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

67. The foregoing frameworks are existing and applicable industry standards in the mortgage industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

68. Defendant's failure to comply was directly contrary to the representations made to its customers in tits Privacy Policy and constitutes materials misrepresentations.

F. Defendant's Breach

69. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow, and intentionally misrepresented to them the actions that it would take to protect their confidential information. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. failing to adequately protect PII;

c. failing to properly monitor their own data security systems for existing intrusions;

d. failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

j. failing to train all members of their workforces effectively on the policies and procedures regarding PII;

k. failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

m. failing to adhere to industry standards for cybersecurity as discussed above; and,

n. otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII.

70. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and

Class Members' PII by allowing cyberthieves to access Defendant's online loan application flow, which provided unauthorized actors with unsecured and unencrypted PII.

71. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

72. Cyberattacks and data breaches at mortgage companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

73. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

74. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a

[10] *See* U.S. GOV. ACCOUNTING OFFICE, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) https://www.gao.gov/new.items/d07737.pdf.

hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

75. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

76. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

77. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

78. Moreover, theft of PII is also gravely serious because PII is an

[11] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited Feb. 23, 2023).

extremely valuable property right.[12]

79. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

80. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

81. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

82. PII is such a valuable commodity to identity-thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

83. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity

---

[12] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[13] GAO Report, at p. 21.

theft for many years into the future.

84. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

85. PII can sell for as much as $363 per record according to the Infosec Institute.[14] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

86. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[15] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[16] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

87. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to

[14] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[15] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 23, 2023).

[16] *Id* at 4.

link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

88. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

89. Because of the value of its collected and stored data, the mortgage industry has experienced disproportionally higher numbers of data theft events than other industries.

90. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

91. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to

[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

92. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

93. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[19]

94. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

95. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and

[19] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm,* Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance- finn/

identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

96. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

97. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

H. Data Breaches Are Preventable.

98. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[20]

99. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like

[20] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[21]

100. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities

[21] *Id.* at 3-4.

- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[22]

101. Given that Defendant was storing the sensitive PII of its current and former customers and applicants, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

I. Plaintiffs' and Class Members' Damages

102. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

103. Defendant LDI has merely offered Plaintiffs and Class Members complimentary fraud and identity monitoring services for up to two years, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

104. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach.

105. Plaintiffs and Class Members' full names, addresses, tax identification numbers, and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software

[22] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

maintaining PII. This PII was acquired by some unauthorized, unidentified third-party threat actor.

106. Since being notified of the Data Breach, Plaintiffs has spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

107. Due to the Data Breach, Plaintiffs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

108. Plaintiffs' PII was compromised as a direct and proximate result of the Data Breach.

109. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

110. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

111. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

112. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

113. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

114. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

115. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's systems and Plaintiffs' and Class Members' PII. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

116. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

117. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. purchasing credit monitoring and identity theft prevention;

c. placing "freezes" and "alerts" with reporting agencies;

d. spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. contacting financial institutions and closing or modifying financial accounts; and

f. closely reviewing and monitoring Social Security numbers,

medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

118. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

119. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

120. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

J. Plaintiffs' Experiences

Plaintiff Schmidt

121. Plaintiff Schmidt applied for a loan from Defendant in or about November 2023.

122. As a condition of submitting his loan application, Plaintiff was required to provide his sensitive PII to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

123. Plaintiff Schmidt is very careful about sharing his sensitive PII. Plaintiff Schmidt has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

124. Plaintiff Schmidt first learned of the Data Breach after receiving a data breach notification letter dated July 31, 2023, from LDI, notifying him that Defendant suffered a data breach a month prior and that his PII had been improperly

accessed and acquired by unauthorized third parties while in possession of Defendant, including his name, date of birth, address, and Social Security number.

125. As a result of the Data Breach, Plaintiff Schmidt made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching and verifying the legitimacy of the Data Breach and contacting Defendant to obtain more details about its occurrence. Plaintiff Schmidt has spent multiple hours and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

126. Plaintiff Schmidt suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

127. Plaintiff further suffered actual injury in the form of his PII being disseminate don the dark web, according to Verizon, which, upon information and belief, was caused by the Data Breach.

128. As a result of the Data Breach, Plaintiff Schmidt has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Schmidt is very concerned about identity theft and fraud, as

well as the consequences of such identity theft and fraud resulting from the Data Breach.

129. As a result of the Data Breach, Plaintiff Schmidt anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

Plaintiff Jantzen

130. Plaintiff Jantzen is a current customer at Defendant and has been since approximately 2021.

131. As a condition of receiving services at Defendant, Plaintiff was required to provide his sensitive PII to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

132. Plaintiff Jantzen is very careful about sharing his sensitive PII. Plaintiff Jantzen has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

133. Plaintiff Jantzen first learned of the Data Breach after receiving a data breach notification letter dated July 31, 2023, from LDI, notifying him that Defendant suffered a data breach a month prior and that his PII had been improperly accessed and acquired by unauthorized third parties while in possession of Defendant.

134. As a result of the Data Breach, Plaintiff Jantzen made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Jantzen has spent multiple hours and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

135. Plaintiff Jantzen suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

136. As a result of the Data Breach, Plaintiff Jantzen has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Jantzen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

137. As a result of the Data Breach, Plaintiff Jantzen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

CLASS ACTION ALLEGATIONS

138. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

139. Plaintiffs propose the following Class and Subclass definitions, subject to amendment as appropriate:

Nationwide Class

All persons in the United States identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

Florida Subclass

All persons in the state of Florida identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Florida Subclass").

140. Excluded from the Classes are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

141. Plaintiffs reserve the right to amend or modify the Class and/or Florida Subclass definitions as this case progresses.

142. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

143. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and

scope of the information compromised in the Data Breach;

c. if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. if Defendant owed a duty to Class Members to safeguard their PII;

f. if Defendant breached their duty to Class Members to safeguard their PII;

g. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendant should have discovered the Data Breach sooner;

i. if Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. if Defendant's conduct was negligent;

k. if Defendant's breach implied contracts with Plaintiffs and Class Members;

l. if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

144. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

145. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

146. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

147. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

148. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

149. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. if Defendant failed to timely notify the public of the Data Breach;

b. if Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. if Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. if Defendant's failure to institute adequate protective security measures amounted to negligence;

e. if Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. if adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

150. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant LDI.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

151. Plaintiffs re-allege and incorporate by reference herein all allegations contained in the foregoing paragraphs.

152. Plaintiffs and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

153. Defendant has full knowledge of the sensitivity of the PII and the types

of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

154. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

155. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

156. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

157. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

158. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

159. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential PII.

160. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. failing to adequately monitor the security of their networks and systems;

d. failing to have in place mitigation policies and procedures;

e. allowing unauthorized access to Class Members' PII;

f. failing to detect in a timely manner that Class Members' PII had been compromised; and

g. failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

161. Defendant owed to Plaintiffs and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

162. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class

Members.

163. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

164. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and Class Members' PII.

165. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

166. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it.

167. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class Members—which actually and proximately caused the Data Breach and injured Plaintiffs and Class Members.

168. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiffs and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

169. Defendant's breach of its common-law duties to exercise reasonable

care and their failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On behalf of the Plaintiffs and the Class)

170. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

171. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

172. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

173. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

174. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

175. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

176. Defendant knowingly did not notify Plaintiffs and Class Members in a

timely fashion about the Data Breach.

177. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

178. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

179. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

180. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

181. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

182. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

183. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

184. Defendant published its "Privacy Policy" to Plaintiffs and the Class as

customers on its website In that policy, and Defendant promised, as consideration to customers providing private and sensitive PII to take appropriate steps to safeguard personally identifiable information by implementing industry standard physical, electronic, and operational policies and practices.

185. Defendant further represented, and continue to represent as further consideration that it had implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in Defendant's possession, to guard against unauthorized access, and that it would continue to assess new technology as it becomes available and to upgrade its physical and electronic security systems as appropriate.

186. These promises by Defendant constituted an implied contract between Defendant and Plaintiffs and Class Members Defendant breached these implied contracts by failing to provide the promised adequate security to protect the private and sensitive PII from disclosure t third parties. Defendant had notice and knew that its cybersecurity practices were inadequate would cause injury to Plaintiffs and the Class.

187. As a proximate result of Defendant's breach of contract the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

188. Defendant's continue to breach and cause injury great to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

189. Plaintiffs, on behalf of themselves and Class Members, seek actual and consequential compensatory damages for Defendant's breach of contract, which includes the value of the privacy interest disclosed by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

190. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

191. This count is pleaded in the alternative to breach of implied contract above.

192. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

193. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

194. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

195. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

196. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering financial services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' PII, and by providing Defendant with their valuable PII.

197. Defendant was enriched by saving the costs they reasonably should

have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid the data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

198. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

199. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

200. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

201. Plaintiffs and Class Members have no adequate remedy at law.

202. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued

possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

203. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

204. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
Violation of the California Unfair Competition Law
[Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices]
(On Behalf of Plaintiffs and the Class)

205. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

206. LDI violated Cal. Bus. and Prof. Code § 17200, et seq., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

207. LDI engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' PII in an unsecure electronic environment in violation of

California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires LDI to take reasonable methods for safeguarding the PII of Plaintiffs and the Class Members.

208. In addition, LDI engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

209. As a direct and proximate result of LDI's unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by LDI for the products and services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

210. LDI knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was highly likely. LDI's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

211. Plaintiffs, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that LDI may have acquired by means of its unlawful, and unfair business practices, disgorgement of all profits accruing to LDI because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

SIXTH CAUSE OF ACTION
Violation of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiff Schmidt and the Florida Subclass)

212. Plaintiff Schmidt ("Plaintiff for the purposes of this count) re-alleges and incorporates by reference herein all of the allegations contained in the foregoing

paragraphs and brings this claim on behalf of himself and the Florida Subclass (the "Class" for the purposes of this count).

213. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained Plaintiff's and Class members' PII through advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiff and Class members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

214. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard Plaintiff'' and Class Members' PII;
b. failure to make only authorized disclosures of customers' and applicants' PII;
c. failure to disclose that their data security practices were inadequate to safeguard customers' PII from theft; and
d. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members.

215. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendant's current and former customers and/or applicants.

216. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Defendant's current and former customers and applicants that they did not follow industry best practices for the collection, use, and storage of PII.

217. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been harmed and have suffered damages including, but not limited to: ((i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) Plaintiffs' PII being disseminated on the dark web, according to Verizon; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

218. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

219. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class members are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendant implement measures that ensure that the PII of Defendant's current and former customers and applicants is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for their provision of services;

c. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response

to a breach; and

d. Ordering Defendant to meaningfully educate its current and former customers and applicants about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

SEVENTH CAUSE OF ACTION
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

220. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

221. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

222. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

223. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

224. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e., Plaintiffs and the Class') data.

225. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

226. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

227. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Class and Florida Subclass, and appointing

Plaintiffs and their Counsel to represent the Class and Florida Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order;

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of

Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal

identifying information of Plaintiffs and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party

assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

Dated: January 29, 2024

Respectfully submitted,

LARSON LLP

By: /s/ Stephen G. Larson
Stephen G. Larson
Paul A. Rigali

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
John J. Nelson

KOELOWITZ OSTROW P.A.
Jeff Ostrow*

THE CONSUMER PROTECTION FIRM, PLLC
William "Billy" Billy Peerce Howard *
Amanda J. Allen *

Attorneys for Plaintiffs and Proposed Class

* PHV Pending

JURY TRIAL DEMANDED

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: January 29, 2024

Respectfully submitted,

LARSON LLP

By: /s/ Stephen G. Larson
Stephen G. Larson
Paul A. Rigali

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
John J. Nelson

KOELOWITZ OSTROW P.A.
Jeff Ostrow*

THE CONSUMER PROTECTION FIRM, PLLC
William "Billy" Billy Peerce Howard *
Amanda J. Allen *

Attorneys for Plaintiffs and Proposed Class